UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,369	03/30/2004	Douglas S. Ransom	6270/139	4719

46260 7590 02/27/2009

BRINKS HOFER GILSON & LIONE/PML
PO BOX 10395
CHICAGO, IL 60610

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
02/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,369	RANSOM ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *42-82* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *42-46,49,51-69,72,74-79,81 and 82* is/are rejected.

7)☒ Claim(s) *47,48,50,70,71,73 and 80* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This non-final action is in response to the Request for Continued Examination filing of 12/12/2008. Claims 42-82 are pending and have been considered as follows.

Examiner Note

In light of the applicants' remarks and amendments, the examiner hereby withdraws his previous Claim Objections with respect to Claims 1, 32, & 41, as the cancellation of these Claims now renders the previous Objection moot.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 42-46, 49, 51, 52, 55-69, 72, 74-79, 81, & 82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Selph et al. (US-4804957-A) in view of Shear et al. (US-6157721-A).

Claim 42:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network comprising,

- "an energy distribution system interface configured to couple said energy management device with at least a portion of said energy distribution system" (i.e. "The electric utility service enters through service drop cable 28, which may include one or more hot conductors and neutral. The electric utility service enters riser conduit 24, passes through socket 22 and enters the building structure through entrance cable 30") [column 5 12-16];
- "a network interface configured to couple said energy management device with said network for transmitting outbound communications to said network" (i.e. "Meter interface unit 36 is coupled to meter 20 and provides communication between the meter and the commercial telephone network") [column 5 lines 35-37];
- "said outbound communications comprising energy management data" (i.e. "The electrical readout signals from meters 38 and 40 are delivered to the utility meter 20 of the invention through connection lines 42") [column 5 lines 49-55];
- "a processor coupled with said network interface and said energy distribution system interface, configured to generate said energy management data" [Fig 6A illustrates a processor interfaced with various components associated with the meter];
- "an enclosure which surrounds said energy management device and protects said energy management device from tampering" (i.e. "The invention is housed in an enclosure which prevents physical tampering with the electronic circuitry") [column 3 lines 35-36];
- "a tamper prevention seal coupled with said enclosure, which detects unauthorized access to said enclosure" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor") [column 3 lines 39-40];

- "a seal tamper detection unit coupled with said processor and said tamper prevention seal and configured to detect when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44];

but, they do not explicitly disclose,

- "wherein said processor is further configured to maintain said energy management data, but prevent said transmitting of said energy management data through said network interface, when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting the processing environment, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein said processor is further configured to maintain said energy management data, but prevent said transmitting of said energy management data through said network interface, when said seal tamper detection unit detects that said tamper prevention

seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. for the purposes of providing a mechanism for protection of the integrity of the processing environment.

Claim 43:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "said tamper seal comprises a revenue seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 44:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "said tamper seal comprises a metering point id seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 45:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "a memory coupled with said processor, said memory configured to store confidential data" (i.e. "A memory, such as a random access memory, is coupled to the processor for storing the digital information") [column 2 lines 62-64].

Claim 46:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 45 above, but Selph et al. do not explicitly disclose,

- "said processor is further configured to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access suggests preventing access.

Claim 49:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 45 above, but Selph et al. do not explicitly disclose,

- "said confidential data comprises a certificate configured to sign said energy management data," although Shear et al. do suggest using digital signatures, as recited below;

however, Shear et al. do disclose,

- "Protected processing environments 108 can use this digital "seal of approval" 106 (which may comprise one or more "digital signatures") to distinguish between authorized and unauthorized load modules 54" [column 9 lines 52-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said confidential data comprises a certificate configured to sign said energy management data," in the invention as disclosed by Selph et al. since digital signatures are a common form of certification to distinguish between authorized and unauthorized information.

Claim 51:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "said processor is further configured to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized

access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 52:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, but Selph et al. do not explicitly disclose,

- "said processor is further configured to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 55:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "said processor is further configured to set off a security alarm when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 56:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "a display coupled with said processor and configured to visually display text" (i.e. "A display, such as an LED or liquid crystal 7 segment display, is responsive to the

processor and provides a visual indication of the digital information provided by the processor") [column 2 lines 67-68];

- "wherein said processor is further configured to place a warning message on said display when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "to provide an alarm event indication in response to a predetermined fault condition") [column 3 lines 17-18].

Claim 57:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "said seal tamper detection unit further comprises a sensor configured to detect that said tamper prevention seal is broken" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor") [column 3 lines 39-40].

Claim 58:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 57 above, their combination further comprising,

- "said sensor comprises a limit switch" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 59:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 57 above, their combination further comprising,

- "said sensor comprises a proximity sensor" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 60:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 59 above, their combination further comprising,

- "said proximity sensor comprises at least one of a pin, an optical proximity sensor, an optical motion detector, a grounding tab, an ultrasonic sensor, an electro-magnetic sensor and a gyroscope" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 61:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 57 above, their combination further comprising,

- "said sensor comprises at least one of a camera and a video camera" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 62:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "an energy storage device coupled with said seal tamper detection unit and configured to provide power to said seal tamper detection unit in power outage situations" (i.e. "a backup power source comprising a storage battery and a low battery detection circuit") [column 3 lines 30-32].

Claim 63:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "said processor is further configured to perform at least one energy management function on said at least a portion of said energy distribution network via said energy distribution system interface" (i.e. "As will be explained in detail below, meter 20 measures the magnetic field generated by the incoming electric current. Entrance cable 30 enters building structure 26 for attachment to a distribution panel 27 with fuses or circuit breakers in the usual fashion") [column 5 16-21];
- "said processor further operative to generate said energy management data as a function of said energy management function" (i.e. "As will be explained in detail below, meter 20 measures the magnetic field generated by the incoming electric current. Entrance cable 30 enters building structure 26 for attachment to a distribution panel 27 with fuses or circuit breakers in the usual fashion") [column 5 16-21].

Claim 64:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, their combination further comprising,

- "an enclosure defining an interior and an exterior and configured to enclose said energy management device within said interior and to limit access to said energy management device" (i.e. "The invention is housed in an enclosure which prevents physical tampering with the electronic circuitry") [column 3 lines 35-36];
- "said tamper prevention seal is coupled with said enclosure and configured to deter unauthorized access to said interior of said enclosure and indicate any such access" (i.e. "The enclosure includes a tamper detection device associated with the housing and

coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-40].

Claim 65:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network comprising,

- "an energy distribution system interface configured to couple said energy management device with at least a portion of said energy distribution system" (i.e. "The electric utility service enters through service drop cable 28, which may include one or more hot conductors and neutral. The electric utility service enters riser conduit 24, passes through socket 22 and enters the building structure through entrance cable 30") [column 5 12-16];
- "a network interface configured to couple said energy management device with said network for transmitting outbound communications to said network" (i.e. "Meter interface unit 36 is coupled to meter 20 and provides communication between the meter and the commercial telephone network") [column 5 lines 35-37];
- "said outbound communications comprising energy management data" (i.e. "The electrical readout signals from meters 38 and 40 are delivered to the utility meter 20 of the invention through connection lines 42") [column 5 lines 49-55];
- "a processor coupled with said network interface and said energy distribution system interface, configured to generate said energy management data" [Fig 6A illustrates a processor interfaced with various components associated with the meter];

- "an enclosure which surrounds said energy management device and protects said energy management device from tampering" (i.e. "The invention is housed in an enclosure which prevents physical tampering with the electronic circuitry") [column 3 lines 35-36];
- "a tamper prevention seal coupled with said enclosure, which detects unauthorized access to said enclosure" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor") [column 3 lines 39-40];
- "a seal tamper detection unit coupled with said processor and said tamper prevention seal and configured to detect when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44];

but, they do not explicitly disclose,

- "wherein said processor is further configured to maintain said energy management data, but configured to mark said energy management data as unreliable, when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting the processing environment, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the

defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein said processor is further configured to maintain said energy management data, but configured to mark said energy management data as unreliable, when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. for the purposes of providing a mechanism for protection of the integrity of the processing environment.

Claim 66:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 65 above, their combination further comprising,

- "said tamper seal comprises a revenue seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 67:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 65 above, their combination further comprising,

- "said tamper seal comprises a metering point id seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 68:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 65 above, their combination further comprising,

- "a memory coupled with said processor, said memory configured to store confidential data" (i.e. "A memory, such as a random access memory, is coupled to the processor for storing the digital information") [column 2 lines 62-64].

Claim 69:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 68 above, but Selph et al. do not explicitly disclose,

- "said processor is further configured to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access suggests preventing access.

Claim 72:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 68 above, but Selph et al. do not explicitly disclose,

- "said confidential data comprises a certificate configured to sign said energy management data," although Shear et al. do suggest using digital signatures, as recited below;

however, Shear et al. do disclose,

- "Protected processing environments 108 can use this digital "seal of approval" 106 (which may comprise one or more "digital signatures") to distinguish between authorized and unauthorized load modules 54" [column 9 lines 52-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said confidential data comprises a certificate configured to sign said energy management data," in the invention as disclosed by Selph et al. since digital signatures are a common form of certification to distinguish between authorized and unauthorized information.

Claim 74:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 65 above, their combination further comprising,

- "said processor is further configured to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 75:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 65 above, but Selph et al. do not explicitly disclose,

- "said processor is further configured to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108

securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 76:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 65 above, their combination further comprising,

- "an energy storage device coupled with said seal tamper detection unit and configured to provide power to said seal tamper detection unit in power outage situations" (i.e. "a backup power source comprising a storage battery and a low battery detection circuit") [column 3 lines 30-32].

Claim 77:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network comprising,

- "an energy distribution system interface configured to couple said energy management device with at least a portion of said energy distribution system" (i.e. "The electric utility

service enters through service drop cable 28, which may include one or more hot conductors and neutral. The electric utility service enters riser conduit 24, passes through socket 22 and enters the building structure through entrance cable 30") [column 5 12-16];

- "a network interface configured to couple said energy management device with said network for transmitting outbound communications to said network" (i.e. "Meter interface unit 36 is coupled to meter 20 and provides communication between the meter and the commercial telephone network") [column 5 lines 35-37];
- "said outbound communications comprising energy management data" (i.e. "The electrical readout signals from meters 38 and 40 are delivered to the utility meter 20 of the invention through connection lines 42") [column 5 lines 49-55];
- "a processor coupled with said network interface and said energy distribution system interface, configured to generate said energy management data" [Fig 6A illustrates a processor interfaced with various components associated with the meter];
- "an enclosure which surrounds said energy management device and protects said energy management device from tampering" (i.e. "The invention is housed in an enclosure which prevents physical tampering with the electronic circuitry") [column 3 lines 35-36];
- "a tamper prevention seal coupled with said enclosure, which detects unauthorized access to said enclosure" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor") [column 3 lines 39-40];
- "a seal tamper detection unit coupled with said processor and said tamper prevention seal and configured to detect when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated

with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44];

- "a memory coupled with said processor and configured to store at least one device setting" (i.e. "During normal operation, microprocessor 138 executes a programmed set of instructions (contained within internal memory or optionally within program memory 158)") [column 10 lines 18-21];

but, they do not explicitly disclose,

- "wherein information of said at least one device setting is preserved when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein information of said at least one device setting is preserved when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. for the purposes of providing a mechanism for protection of the integrity of the processing environment.

Claim 78:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 77 above, but Selph et al. do not explicitly disclose,

- "said processor is further configured to prevent changes to said at least one device setting after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to prevent changes to said at least one device setting after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access suggests preventing access.

Claim 79:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 77 above, their combination further comprising,

- "said processor is further configured to permit changes to said at least one device setting, and further is configured to send a message warning that said device setting has been changed through said network interface after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 81:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 77 above, their combination further comprising,

- "said tamper seal comprises a revenue seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 82:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 77 above, their combination further comprising,

- "said tamper seal comprises a metering point id seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

3. Claim 53 & 54 is rejected under 35 U.S.C. 103(a) as being unpatentable over Selph et al. (US-4804957-A) in view of Shear et al. (US-6157721-A) and in view of Schneier et al. (US-5978475-A).

Claims 53 & 54:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 42 above, but Selph et al. do not explicitly disclose,

- "said processor is further configured to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access

has occurred," although Shear et al. do suggest the common usage of audit logs, as recited below;

- "said processor is further configured to at least one of hash and encrypt said audit log," although Schneier et al. do suggest the usage of message digests for resistance against attacks, as recited below;

however, Shear et al. do disclose,

- "Audit logs have long been used to keep permanent records of critical events. The basic idea is that the audit log can be used at some future date to reconstruct events that happened in the past. This reconstruction might be required for legal purposes (to determine who did what when), for accounting purposes, or to reconstruct things after a disaster: errors, loss of data, deliberate sabotage, etc" [column 1 lines 1-10];

whereas, Schneier et al. do disclose,

- "In the FIG. 5 process, load module 54 (along with specifications 110 if desired) is processed to yield a "message digest" 116 using a conventional one-way hash function selected to provide an appropriate resistance to algorithmic attack" [column 13 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" and "said processor is further configured to at least one of hash and encrypt said audit log," in the invention as disclosed by Selph et al. for the purposes of keeping secure records.

Allowable Subject Matter

4. Claims 47, 48, 50, 71, 71, 73, & 80 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

5. Applicant's arguments with respect to claims 42-82 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicants' amendments.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Butturini et al. (US-7007171-B1) - tamper enclosure and detection seal erasing keys;

b. Benson et al. (US-20020002683-A1) - tamper enclosure and detection circuit erasing sensitive programs/data;

c. Sears (US-5719564-A) - similar elements;

d. Herbert et al. (US-6515574-B1) - tamper detection;

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
02/26/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436